



Steve Jobs and his legacy
in the enterprise. Page 6▶

NETWORKWORLD

THE CONNECTED ENTERPRISE

OCTOBER 10, 2011

VOLUME 28 NUMBER 17 \$5.00



**PUBLIC CLOUD
SECURITY**

MISSION IMPOSSIBLE?

Networkworld.com

**Store and manage your data dynamically and efficiently
with Fluid Data from Dell.**

Fluid Data storage from Dell will help you succeed in the virtual era. Whether you plan to leverage the flexibility of a virtualized data center, optimize critical applications, or shift toward a private cloud, Dell has the experience and products to deliver innovation and cost savings. Our portfolio of award-winning products, including Compellent, EqualLogic and PowerVault, enables you to create fully optimized data storage and save you up to 80% on storage costs. Learn more at DellStorage.com/GetFluid.



The power to do more

21

**Fluid Data
always knows
the most efficient
way to get where
it needs to go.**

23

FROM THE EDITOR | JOHN DIX

All hail OpenStack

The OpenStack collaborative industry effort to build an open source cloud platform is to be applauded for the remarkable gains it has achieved in a short amount of time. Founded by Rackspace Hosting and NASA in July last year, the organization is now backed by 120 companies, including HP, Dell, Intel and Cisco, and has already issued four major code releases, the last of which, Diablo, came out last month and has been downloaded 50,000 times.

Some 600 OpenStack faithful were in Boston last week at a weeklong conference, the first three days of which was a design summit for developers working on Essex, the next release due out in April.

This is a wildly enthusiastic group brimming with people who like to say they are out to change the world. "From day one, OpenStack has been 10 times bigger than we ever expected," says Lew Moorman, Rackspace's chief strategy officer and president of its cloud business. Moorman used the conference to announce plans to create the OpenStack Foundation, which will take over governance of the movement and its intellectual property, a shift that is needed to keep up the momentum.

OpenStack co-founder and former CTO of NASA, Chris Kemp, now CEO of startup Nebula, says the goal is to achieve a common cloud platform for service providers and enterprises that will ensure cloud interoperability, workload portability and development of common tools.

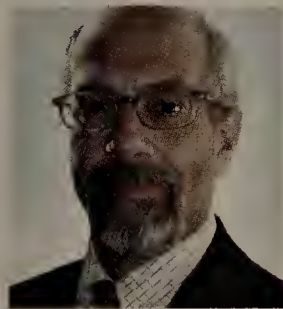
Lofty goals, but the movement is attracting the backing that might just make it possible. "HP is completely onboard with OpenStack," said John Purrier, vice president of HP Cloud Services. The company, which is standing up a 1,000 node OpenStack-based public cloud with several petabytes of storage, launched a private beta of that cloud last month and will go into public beta next year.

Some users are already plowing ahead. MercadoLibre, a giant e-commerce site in Latin America, has 5,000 of its 6,000 virtual server instances running on OpenStack, says Infrastructure Senior Engineer Alejandro Comisario. Other buyers on hand to discuss OpenStack plans included Sony and CERN.

The movement, however, still faces major challenges, chief among them fragmentation of this large undertaking. "The group has to figure out how much effort is spent going wide vs. focusing and getting good at a few things," said Blake Yeager, the lead product manager for IaaS at HP Cloud Services. HP would prefer the latter, he said, "getting the basics rock solid."

A user attending one panel discussion complained that "there is a fair amount of chaos in the delivery. . . . What is needed is a good roadmap about where this is going to be in six months so I can sell it internally."

The next 12 months will determine if OpenStack is a flash in the pan or a sustainable movement.



A handwritten signature of John A. Dix.

6 Trend Analysis

How Apple conquered enterprise mobility.
BY JOHN COX

8 Trend Analysis

Feds want uber cybersecurity standards.
BY TIM GREENE

10 Trend Analysis

Huawei gunning for Cisco in the enterprise.
BY JIM DUFFY

14 Tool Shed Gearhead

Putting the QNAP T-1079 Pro NAS to the test.
BY MARK GIBBS

16 Cool Tools

Lenovo ThinkPad Tablet a business contender.
BY KEITH SHAW

18 Special Edition Enterprise Cloud Services:

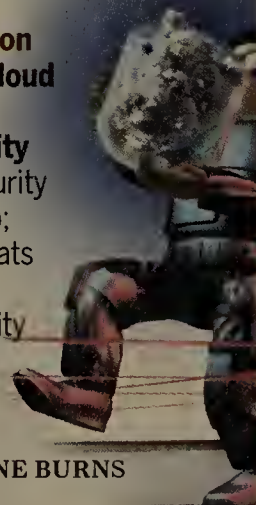
Cloud Security
Essential security tips (page 22);
Looming threats (page 24);
5 cloud security companies to watch (page 30).
BY CHRISTINE BURNS

34 BackSpin

IT ... as Steve said: 'Click. Boom. Amazing!'
BY MARK GIBBS

34 Net Buzz

3 small items from the week we lost a giant.
BY PAUL MCNAMARA



Quantum insights

➔ **MAE-WAN HO ARGUES** in "The Rainbow and the Worm: The Physics of Organisms" that biological cells are already quantum coherent devices. They do this by structuring water into 3D dipolar lattices using alternating positive and negative charges on the surfaces of proteins (this is also discussed in the cell biology book "Cells, Gels and the Engines of Life" by Gerald Pollack). It appears that an important purpose of proteins is to create this structured water. Pollack explains that this structuring of water within the cell lends it all of the characteristics of a gel. The secret to life in the universe is that it is a self-stable system of gel components, where each gel can perform its own functionality by virtue of its inherent, natural phase transitions. These transitions are like living transistors in that they occur very rapidly, and sometimes with tiny triggers (Re: "Is Quantum Computing real?" tinyurl.com/3p3rxlo).

If Pollack and Ho are right, then researchers are wasting time on decoherence. They should simply learn the emerging cell biology framework and copy it, using polymers. This is going to confuse the public, because these systems will in a sense be living. But it does appear that the fields of quantum computing and cell biology are on the verge of combining.

Hugh G

New iPhone over-hyped

➔ **SO MUCH HYPE**, so little delivered today.

Apple is now playing catchup to the 'droids — only the voice feature is better, every other one is last month's news (Re: "Apple unveils iPhone 4S"; tinyurl.com/3fnnjrq). It has always been the OS that set Apple products apart. The phone has not had the big OS improvements and Android has passed iPhone on the feature set. This is not a new-generation phone but a polish of the current one. It will now be a war of Bionic vs. 4S, with Samsung screaming, "Hey, we got the biggest screen." Apple had a chance to leapfrog ahead — but only gets the lead by a nose.

Mike Jandebeur

Amazon lights a Fire

➔ **BASED ON THIS** story Amazon seems to have learned from the failure of other Android tablets. It plans to create an environment for its tablet much like Apple has done. This is important for tablet owners. They want a product that is going to work out of the box. If Amazon works to create a positive user experience it may become the dominant player in the Android market (Re: "Amazon's new tablet: What to expect"; tinyurl.com/4x3pbo4).

I use the Kindle software on my iPad, iPod Touch and MacBook. It seems to work well and is well-designed. If Amazon is able to transfer that quality to its tablet experience it is likely to excel.

justinwachin

➔ **AT \$200, I'LL** get one, even though my wife and I already have iPad 2s (Re: "Tablet Throwdown: Amazon Kindle Fire vs. Apple iPad 2"; tinyurl.com/3w6gx3b). It'll be nice just to have a device laying around the living room. I won't even set up the email app, it'll just be for guests and occasional surfing — no personal info on

it. iPad is too expensive for that, but at \$200 it's feasible. Also could make a great gift for kids, older parents, etc.

compudude

Spectrum auction system failure

➔ **THE SPECTRUM AUCTION** system has created spectrum hogs. The process encourages large bids and the winner must then gouge the cost back from users

(Re: "Citigroup questions if U.S. spectrum shortage exists"; tinyurl.com/5ve86ta).

What if roads were sold off and people had to pay tolls for their use? We'd have a huge number of fragmented pathways. To avoid the tolls, people would go across town and back just to go next door — as now happens with various data paths.

We need the feds to reclaim the spectrum and then make all users share it with standards of equipment — much like we have road standards — and charge a small fee per second or other bandwidth use measure.

Bill Jackson

It will now be a war of **Bionic vs. 4S**, with Samsung screaming, "Hey, we got the biggest screen."

492 Old Connecticut Path, P.O. Box 9002

Framingham, MA, 01701-9002

Main Phone: (508) 766-5301

E-mail: firstname.lastname@nww.com

Editorial Calendar: <http://tinyurl.com/39sf649>

EDITORIAL

Editor in Chief: John Dix

Online Executive Editor, News: Bob Brown

Executive Online Editor: Jeff Caruso

Executive Features Editor: Neal Weinberg

Community Editor: Julie Bort

Multimedia Programming Director: Keith Shaw

NEWS EDITORS

Online News Editor: Michael Cooney

Online News Editor: Paul McNamara

Online Associate News Editor: Ann Bednarz

REPORTERS

John Cox, Senior Editor

Jim Duffy, Managing Editor

Tim Greene, Senior Editor

Carolyn Duffy Marsan, National Correspondent

Ellen Messmer, Senior Editor

Brad Reed, Senior Writer

PRINT LAYOUT/WEB PRODUCTION

Managing Editor: Ryan Francis

Web Producer: Melissa Andersen

DESIGN

Executive Art Director: Mary Lester

Associate Art Director: Stephen Sauer

NETWORK WORLD LAB ALLIANCE

Joel Snyder, Opus One; John Bass, Centennial Networking

Labs; Barry Nance, independent consultant; Thomas

Henderson, ExtremeLabs; David Newman, Network

Test; James Gaskin, Gaskin Computing Services; Craig

Mathias, FarPoint Group

OFFICE MANAGEMENT

Editorial Operations Manager: Cheryl Crivello

Office Manager, Editorial: Pat Josefek

SUBSCRIPTIONS

Phone: (877) 701-2228

E-mail: nww@omeda.com

URL: www.subscribenww.com

REPRINTS

800-290-5460, ext 100

Email: networkworld@theygsgroup.com

IDG Enterprise

An IDG Communications Company

IDG ENTERPRISE

CEO: Mike Friedenber

Group Publisher: Bob Melk

Chief Content Officer/SVP: John Gallant



NETWORK
SECURITY



SECURE
REMOTE ACCESS



WEB AND E-MAIL
SECURITY



BACKUP AND
RECOVERY



POLICY AND
MANAGEMENT

WHO MAKES THE HIGHEST PERFORMANCE LOW LATENCY NEXT-GEN FIREWALL?



SONICWALL
SECURES THE
ENTERPRISE.

SonicWALL® enables IT to get back in control and more easily and efficiently stay ahead of today's constantly evolving threats and application-related issues. An advanced security platform consolidates core Next-Gen Firewall application intelligence, control and visualization, gateway protection, and inspection for SSL encrypted sessions for enterprises along with WAN acceleration for distributed offices. SonicWALL's low latency platform scans and secures every packet of every protocol, efficiently securing the network, controlling Web 2.0 apps, and optimizing bandwidth.

Secure network optimization that minimizes complexity and latency is now within reach. Learn about our SuperMassive® E10000 Series and the rest of our network security line-up at sonicwall.com/optimize.

SONICWALL

How Apple conquered enterprise mobility

It all began with the iPod — then came the iPhone and iPad

BY JOHN COX

WHEN APPLE'S then-CEO Steve Jobs unveiled the iPod 10 years ago this month, no one, including him, could predict that it would pave the way for Apple to dominate the emerging mobile enterprise. How it did so reveals Jobs' true legacy: not Apple's products, but Apple itself.

Just a few years ago, it was rare to find an Apple Mac laptop or desktop anywhere in America's biggest companies. Yet today, according to Apple, more than 90% of the biggest companies in America are deploying or at least testing Apple products, specifically the iOS-based mobile devices, the iPhone and iPad, and doing so in large numbers. The two products are transforming mobility in the enterprise, and the iPhone 4S introduced this week promises continued transformation.

"Four years ago, what percentage of these [companies] had any kind of corporate relationship with Apple?" asks Dan Kerzner, senior vice president of mobile for MicroStrategy, a business intelligence software vendor. "I would contend it was very small."

Today about 2,300 of MicroStrategy's employees have an iPad, and many also have an iPhone. In many — but not all — cases, the Apple tablet has replaced a Windows notebook PC. And the mobile devices are chang-

ing the way MicroStrategy employees work. that Apple created by patiently forging licensing deals with companies — record labels — it had never worked with before. The iPhone and iPad continue those same virtues: the intensely satisfying user experience coupled with a nearly invisible, highly disciplined infrastructure reaching through to OEM suppliers in the Far East, to iOS developers, to the online App Store, to Apple salespeople in retail stores, to tech support staff handling calls from end users.

The enterprise market is one that Apple as a company paid little attention to: There is no complex Apple systems management and virtualization and security infrastructure, so characteristic of Microsoft and others who target enterprise IT. So what accounts for this astounding success?

"The user experience, the ease of use, the graphical displays, along with the usability-based innovations are the primary reason for Apple's success in the enterprise," says Manoj Prasad, vice president of information technologies, with Life Technologies, a Carlsbad, Calif., vendor of biotechnology products for research, with a major iOS deployment.

Abilene Christian University in Abilene, Texas, standardized on the iPhone and iPod Touch — even before there was an App Store — as the technology platform for rethinking and redoing its entire educational curriculum.

Educators there had seen three key trends emerging with students, says William Rankin, associate professor of English and ACU's director of educational innovation.

The trends were the rise of social net-

works, the explosive increase in media (music, photos, video) and the power of the full-blown worldwide Web on mobile devices. In studying students' media usage, for example, the educators saw that students were creating collections of music, one for "my rainy day mix," another for "my chill-out mix," still another for "getting pumped for my final exam mix." "They were creating a soundtrack of their lives, organizing information around their lives," Rankin says.

"Nothing brought these three things together — except the iPhone, and then the iPad," he says. "When we saw that it could unify these three pieces, we knew we could

do anything we wanted."

A similar kind of epiphany has been sweeping corporate America. The first iPhone was released in June 2007. It was roundly criticized for lacking the security and management features that were standard-issue on corporate Windows laptops and RIM BlackBerries, the devices that constituted then the meaning of "enterprise mobility." But the runaway success of the iPhone in successive models, and of the iPad released in spring 2010, was evidence that end-users were redefining that term on their own: bringing the devices to work and clamoring for access to email, applications and data.

"Once they had this easy and fun experience with their [own] mobile device in their consumer life, people couldn't understand why it couldn't be like this for their mobile work life," says Stacy Crook, senior research analyst, mobile enterprise, for market research firm IDC.

With the introduction of iPhone 3GS in June 2009 and even more the June 2010 release of iPhone 4, running the iOS 4 firmware, Apple was steadily adding what was needed for acceptable security and management by many companies, including support for Microsoft Exchange ActiveSync, and the Cisco VPN client. For many other companies, the Apple devices were instantly seen not as toys but as work enablers, the result not just of the simplicity and intuition of the touch interface, but also of their long battery life (eight to 10 hours), and their instant-on, ready-to-go availability.

"My belief is that most people are afraid of computers," says Ken Dulaney, vice president of mobile at Gartner. "Not that they can't do the basics, but they feel stupid that they cannot get more out of the device." He contrasts the "lifestyle" themed advertising of many smartphone rivals with Apple's close-up focus on the iPhone itself. "They show you how you can do things," he says. "Assuaging people's fears is a powerful thing. Apple does it well."

Apple was able to assuage IT fears as well. Securing, managing and supporting the Apple devices compared to Windows notebooks "was not a big change for us," says MicroStrategy's Kerzner. "We had some core [policy] tenets ... and you accept that this is a new form of device and just get on with it," he says. "The tools are all there."

The introduction of APIs to support third-party device management and security applications with iOS 4 was a major step forward.



“The world rarely sees someone who made such a profound impact.”

STEVE WOZNIAK, CO-FOUNDER, APPLE

ing the way MicroStrategy employees work.

At Needham Bank, a small community bank with several branches in the Needham, Mass., area, iOS devices in effect have replaced what used to be the ubiquitous paper notepads and pens. "Everyone is staring at their iPhone or iPad," says James Gordon, the bank's vice president of IT. "Often, meetings are being held here and everyone in the room is using the iPad to digitally consume and discuss that information."

Ten years ago, the iPod created a deceptively simple, focused experience for its owners. But it also leveraged the catalog of music

Steve Jobs tributes

"Steve was among the greatest of American innovators — brave enough to think differently, bold enough to believe he could change the world, and talented enough to do it."

PRESIDENT **BARACK OBAMA**

"People sometimes have goals in life. Steve Jobs exceeded every goal he ever set for himself."

BILL GATES, CHAIRMAN, MICROSOFT

"Steve Jobs did more than simply shape our concepts of technology and invention, he helped define our understanding of how great innovation and design can bring people closer together."

JOHN CHAMBERS, CEO, CISCO

"His focus on the user experience above all else has always been an inspiration to me."

LARRY PAGE, CEO, GOOGLE

"Steve Jobs was the greatest inventor since Thomas Edison. He put the world at our fingertips."

STEVEN SPIELBERG, MOVIE DIRECTOR

"I think he's the greatest entrepreneur we've ever known or seen. Look at what he did with Apple, what he did with Pixar."

SCOTT MCNEALY, FORMER CEO, SUN

Needham Bank relies on MobileIron's application for centralized management and deployment of iOS devices. "We have jailbreak detection and enterprisewide iOS geolocation ability," says IT chief Gordon. "The APIs written for the enterprise have been sufficient for our needs."

But companies are still forced to make adjustments. Life Technologies' Prasad runs through a litany of standards that Apple's mobile products don't currently support: USB, HDMI, Java applets, Adobe Flash and more. "This lack of support makes it difficult for enterprise users to use Apple's mobile devices [with resources that rely on these standards]," he says. The limited functionality on iOS devices of widely used products like Microsoft Office can impact productivity. Adding third-party management tools specifically for iOS means adding costs and complexity.

In a provocative post at *Harvard Business Review*, "Steve Jobs and the Eureka Myth," written just after Jobs resigned as CEO in August, Adrian Slywotzky, a partner of Oliver Wyman,

a global management consulting firm, argued that the idea of Jobs as "an inspired savant who succeeded by taking big risks on personal hunches, is way off the mark."

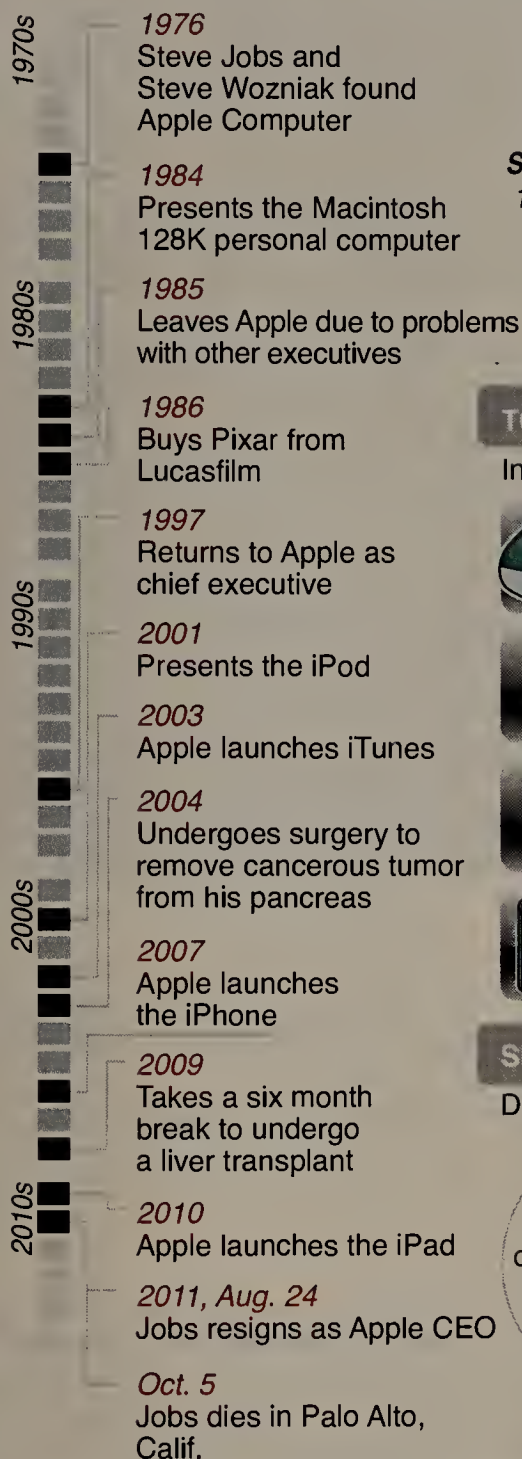
"Apple would love us to believe it's all 'Eureka,'" Slywotzky writes. "But Apple produces 10 pixel-perfect prototypes for each feature. They [then] compete — and are winnowed down to three, then one, resulting in a highly evolved winner. Because Apple knows the more you compete inside, the less you'll have to compete outside."

"We are all mesmerized by Apple's beautiful

design, from device to screen, to the packaging itself. We see what the magicians want us to see. What we don't see is the 18 months of negotiating with the music companies. Nor the three years of teaching the supply chain that the MacBook Air had to be really thin, really light, and really enduring (10-hour battery). When those improvements intersected with the iPhone's great screen technology, the iPad (that glorious Air/iPhone hybrid) exploded."

That explosion is still echoing through the enterprise. ■

Timeline of Steve Jobs at Apple



Steve Jobs
1955-2011



TOP PRODUCTS

Introduction date



May 6, 1998
First iMac, an all-in-one computer, reminiscent of the Macintosh



Oct. 23, 2001
First iPod. Mac OS X released early the same year



Jan. 9, 2007
Jobs unveils the first iPhone



January 2010 The iPad, a touchscreen tablet media device is launched

SHARE PRICE

Daily close in dollars

Sep. 20,

\$413.45

2011, Aug. 9
Apple briefly overtakes Exxon as the world's most valuable company

2011
Oct 05,
\$378.25

\$214.01

December 1980

Apple launches IPO

\$3.59

\$9.31

\$32.58

'85 '90 '95 '00 '05 '10

REUTERS

Feds want uber cybersecurity standards

BY TIM GREENE

TIRED OF regulators from three or four federal agencies auditing your network security compliance every year? A congressional task force recommends a super-standard that would cut the number of annual audits to just one.

If adopted, the proposal would consolidate federal cybersecurity mandates issued by disparate agencies into a single set of standards that would satisfy all of their requirements. Businesses would have to submit to a single audit that would satisfy all requirements, according to the House Republican Cybersecurity Task Force.

The group notes that Sarbanes-Oxley, Health Insurance Portability and Accountability Act and Graham-Leach-Bliley all impose security requirements. "A company would be encouraged to implement stronger security standards by allowing it to save money and time by avoiding multiple audits from multiple regulators," the task force says.

The task force was set up in June by House Speaker John Boehner in part to respond to the Obama administration's proposed cybersecurity legislation, delivered to Congress in May.

Regulatory compliance has become the bane of CIOs and CISOs, sapping their budgets to where some say they can afford to do little else but meet the regulations.

At this week's SINET Innovation Summit in Boston, Sallie Mae CSO Jerry Archer said his agency spent 40% of its budget on complying with regulations. "What is needed is automating compliance to reduce the bite it takes from the budget," he says.

Another speaker at the summit congratulated him on such a low percentage. "For some it's 100%," said Josh Corman, director of security intelligence at Akamai. The trouble with regulations is that they drive security architectures and prevent data loss that may have little real impact, while ignoring thefts that could be devastating.

For instance, loss of credit card numbers — protection of which falls under the private payment card industry standards — is painful to the card holders, but the cards can be replaced. More focus should be put on data breaches that result in the loss of critical technologies that could wipe out businesses or imperil national security, Corman says.

The congressional task force also says that the best way for government to get the big picture of cyberattacks is to have someone else do the investigation.

The task force's recommendations include

Cybersecurity task force proposals

The House Republican Cybersecurity Task Force recommendations on improving the defense of critical infrastructure include the following:

- Create incentives that encourage businesses to adopt voluntary standards for cybersecurity.
- Streamline federal cybersecurity regulations to a single standard.
- Limit liability of businesses that follow the voluntary standards but suffer breaches anyway.
- Broaden the scope of cyber incidents that must be reported.
- Form an extra-governmental cyber-intelligence clearinghouse for government and critical infrastructure players.
- Pass a national data-breach-notification law.

setting up an organization separate from government that gathers data on cyberattacks for government and private groups to tap into when they need a picture of ongoing cyberactivity threatening critical infrastructure.

Government is too slow to respond to ever-changing threats in a timely manner, a problem an independent entity authorized to gather and disseminate attack details wouldn't face, the task force says. "Owners and operators know best how to protect their own systems, and it is nearly impossible for the speed of bureaucracy to keep pace with ever changing threats," the task force says.

The idea of distancing government from cybersecurity decisions that inherently require quick action was echoed this week at the SINET Innovation Summit. The group met to discuss how security technologies that the government needs can be developed and rapidly deployed by quick-moving startups.

One conclusion: Partnerships could be created that pull together funding, research and development, and transition the resulting technology to products that can be developed quickly. Central to this model is

limiting the role of government, says Douglas Maughan of the Department of Homeland Security (DHS).

"Keep government at a distance," Maughan told the group. "Things don't always go so well when the government's in the middle."

He cited the case of the LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) project in which DHS has collaborated with petroleum companies to address issues in that industry. One effort called the Correlation Project involved cooperation of the DHS and private businesses including petroleum giants BP, Chevron and Citgo. The project was coordinated through a third party.

The project came up with a correlation engine that took input from supervisory control and data acquisition (SCADA) systems as well as from corporate business networks and spit out attack warnings, Maughan said.

Other recommendations from the congressional task force call for a set of incentives that encourage businesses to do the right thing when it comes to defending their networks against cyberattacks.

Incentives such as reducing data-breach liability, tax credits, insurance breaks and tying government grants to cyber-compliance should be considered, the task force reports.

Congress should adopt voluntary incentives to encourage better security measures be adopted by private businesses that control critical infrastructure such as power grids, water supplies and fuel supplies. Other businesses would be free to adopt the same standards, the task force says.

When doling out grants to businesses, Congress could require compliance with minimum cybersecurity protection standards if the grants pertain to national security, law enforcement and critical infrastructure, the task force recommends.

Congress should look into whether insurance companies could encourage better cybersecurity among policy holders. The task force didn't seem to know how insurance companies handle this, but recommended finding out.

While generally opposed to mandates, the task force said further regulation may be warranted in cases of industries that control critical infrastructure, but it wants to keep new requirements light.

Businesses directly involved in these critical areas should contribute to developing these additional standards, the report says. In addition, if businesses comply and are breached anyway, their liability should be reduced by virtue of compliance. ■

17,113 students

2,300 employees

73 square miles

25 campuses

One Charter Business® Fiber Solution that offered a smart alternative to critical connection uptime.

When swelling bandwidth demands caused bottlenecks and interruptions, the director of Technology Services at Eagle Mountain-Saginaw School District turned to Charter Business Fiber Solutions for a faster, scalable connection.

With a wholly owned, proactively monitored network backed by an enterprise support team 24/7, we have the intelligence to help schools, healthcare facilities, financial institutions and businesses of every size run at their best.

Fiber Internet
Data Networking
Optical Ethernet
Advanced Voice Solutions

Learn more about this story.



Charter-Business.com/Technology | 888.891.1598

Huawei gunning for Cisco in the enterprise

Forms new group dedicated to sell billions in routers, switches and telepresence

BY JIM DUFFY

THINGS ARE about to get a little hotter for Cisco in the enterprise market.

Huawei, the cut-rate Chinese competitor Cisco fears most, is formalizing its entry into the U.S. and global enterprise market. It's establishing a presence in Silicon Valley, and shifting over and recruiting 10,000 people to staff its new group — one of three main Huawei business units along with Devices and Telecom Infrastructure.

Karen Yu is president of Huawei's Enterprise business in the U.S. The company is recruiting channel partners to market its campus networking, branch access, IP backbone, data center and videoconferencing products.

Three product areas will be a key focus for the new group, however: LAN switches, access routers and telepresence, says John Roese, Huawei's senior vice president and general manager of North American R&D. Huawei, a \$29 billion company, did \$2 billion in enterprise business last year, but by formalizing its enterprise efforts and attacking the North American market in earnest, it's looking to at least double that this year, and more than triple that tally in 2012.

Cisco has dominated the enterprise networking market for a decade or more. Juniper entered the market in 2004 with its NetScreen firewall and VPN acquisition, and then with LAN switches in 2008, but its sales there have been flat of late. HP is the clear No. 2 in LAN switching behind Cisco, and doubled its market share by acquiring 3Com in 2009. But HP is still at about 10% market share, while Cisco enjoys 65% or more.

What makes Huawei different and why now?

Three reasons, according to Roese: 1) the carrier, enterprise and consumer markets are converging, and that plays to Huawei's competencies in each market, he says; 2) there hasn't been a "major new entrant" in a while, even though the market grew substantially; and 3) customers trying to figure out consumerization of IT, the blurring lines between enterprise, carrier and consumer, and how to build extended or virtual enterprise.

"We're entering a market where many of our competitors are a bit complacent," Roese says. "Smaller players are not really strategic threats because they simply are not big enough. Huawei, on the other hand, is clearly big enough."

If Huawei hits that goal of \$7 billion in

“We’re entering a market where many of our competitors are a bit complacent. Smaller players are not really strategic threats because they simply are not big enough. Huawei, on the other hand, is clearly big enough.”

JOHN ROESE, HUAWEI'S SENIOR VICE PRESIDENT AND GENERAL MANAGER OF NORTH AMERICAN R&D



enterprise networking revenue in 2012, it will clearly be the No. 2 player to Cisco, Roese says. The company is looking to be a \$10 billion to \$15 billion enterprise player in the next five years, he says.

He expects most of that business to come at the expense of Cisco rather than that of the HPs, Junipers, or smaller players like his old employers Enterasys and Nortel enterprise, which is now owned by Avaya.

"If we took share from everyone but (Cisco), we wouldn't hit our number," Roese says. "The smaller players could potentially struggle in this environment. When there's true competition among the big players, the big players innovate and go after more of those niches filled by smaller players. It will be tough for the midsize players to meet the scale of the big players."

First, Huawei has its work cut out. It has to cultivate a roster of channel partners and convince them to push a Chinese brand with a checkered past — Huawei was embroiled in patent and intellectual property litigation with Cisco years ago. Huawei's Chinese roots also led to security concerns in the U.S. when it and Bain Capital looked to acquire 3Com years ago. That deal collapsed.

Huawei also has to Westernize its product portfolio and make the user interface a little more familiar to customers in North America, Roese says.

The Chinese and intellectual property issues are well in the past, Roese says.

"We're multinational with a significant presence in China and developing countries," he says. "Most of the global companies that exist have already gotten over their concerns about competing in a global ecosystem. Lots

of verticals in the U.S. are open to a global company, an international company, selling them technology."

He says Huawei over the years has invested "huge resources" into building up its own intellectual property portfolio. It now owns 50,000 patents and has 120 leadership positions in standards bodies around the world, Roese says.

"Clearly, we recognize the value of intellectual property and put a huge amount of resources into making sure we were a have, not a have-not, in this market," he says.

Roese is also confident that the economics of the Huawei channel program will entice partners, and that profit distribution will be "a little bit more equal" for all parties involved versus competitive programs.

One area where Huawei will stay to the sidelines and let the dust settle is in data center fabrics. Huawei already has a unified fabric offering for carriers and service providers, but the company is content to wait a bit before pushing it in the enterprise.

"The idea of a customer making such a radical shift in their data center architecture is such a high risk proposition for an enterprise CIO that this is going to take a long time to progress," Roese says. "Let the war happen, let the customer settle down, let the technology mature. Let competitors kill each other, learn what they did right or wrong. We'll be at a pretty good advantage especially when we're not losing the ability to penetrate the market."

Roese says Huawei's interest is more in cloud architectures "on the outside" and gateways to connect into it through access routers.

Huawei's enterprise headquarters will be split between China and Santa Clara. ■

Microsoft



Streamlined provisioning.
Easy-to-use permissions.
Enterprise-grade security.
It all works together.

Introducing Microsoft Office 365. Collaborate in the cloud with Office, Exchange, SharePoint, and Lync videoconferencing. **Starting as low as \$10 per user per month. Begin your free trial now at Microsoft.com/office365**



Scan tag with a smart-
phone to learn about
the Office 365 free trial.
Download the free
scanner app at
<http://gettag.mobi>

 Microsoft®
Office 365

QUALITY WWW

OFFERING SUPERIOR WEBSITE SEC



1&1 DUAL HOSTING

Best value for your business!

We are dedicated to security, innovation and value when it comes to your website.

- ✓ **Dual Security:**
Your website is simultaneously hosted in 2 locations in our geo-redundant data centers!
- ✓ **High speed Global Network:**
210 GBit/s Connectivity
- ✓ **Environmentally Responsible:**
100% Renewable Energy
- ✓ **Solid Technical Foundation:**
1,000 In-house Developers

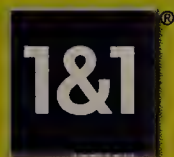


WEB HOSTING

SECURITY WITH 1&1 DUAL HOSTING!

--- HURRY! OFFER ENDS 10/31/2011 --- HURRY! OFFER ENDS 10/31/2011 --- HURRY! OFFER ENDS 10/31/2011 ---

NOW
6 MONTHS
FREE!*



GoDaddy®

Network
Solutions®

Package	1&1 BUSINESS	ULTIMATE	UNLIMITED
Domains	1	0	1
Webpace	unlimited	unlimited	unlimited
Traffic	unlimited	unlimited	unlimited
1-Click Applications	unlimited	unlimited	–
E-mail	unlimited	1,000	unlimited
MySQL	unlimited	unlimited	unlimited
FTP Accounts	unlimited	50	unlimited
Dedicated IP Address	✓	✓	–
Superior Security through 1&1 Dual Hosting	✓	–	–
Programming Language Support	PHP5, PERL, Python, Ruby, Zend	PHP5, PERL, Python, Ruby on Rails	PHP5, Python, Ruby on Rails, Zend
SSL Certificate	1 (forever)	1 (just initial term)	\$ 139.00 (per year)
Set-up Fee	\$ 9.99	–	–
Monthly Cost	~~\$ 9.99~~ 6 MONTHS FREE*	\$ 11.99	\$ 29.13
Annual Cost	\$ 69.93	\$ 143.88	\$ 488.50

1&1 UNLIMITED
NOW
6 MONTHS
FREE*

~~\$ 6.99~~ per month

Visit our website for
more special offers.



Get started today, call **1-877-461-2631**

www.1and1.com

* Offer valid through 10/31/2011. 12 month minimum contract term required. Other terms and conditions may apply. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners. © 2011 1&1 Internet AG. All rights reserved.

TOOLS

Putting the QNAP T-1079 Pro NAS to the test

A couple of weeks ago I started trying to get a QNAP TS-1079 Pro network-attached storage (NAS) device set up. Just to remind you: The QNAP TS-1079 Pro is a desktop-style NAS device that runs an embedded version of Linux on a dual core Intel i3-2120 Processor at 3.3 GHz with 2GB of DDR3 RAM. It has 10 drive bays allowing up to 30TB of storage set up as JBOD (that's "Just a Bunch Of Disks") or in any of the usual RAID configurations.

The TS-1079 Pro is a well connected device; it has two Gigabit Ethernet ports with an optional dual-port 10 Gigabit or 1Gigabit network card along with two eSATA ports, four USB 2.0 ports and two USB 3.0 ports. The device also supports iSCSI, making it VMware, Citrix and Hyper-V ready.

A feature of the TS-1079 Pro I was trying to test is QNAP's MyCloudNAS, essentially a custom Dynamic DNS service for QNAP products. Through a "wizard" accessed on the QNAP device you select a subdomain of MyCloudNAS.com and, if that is available, which services you want to be visible from the Internet.

These services can include both or either unsecured (HTTP) and secured (HTTPS) access to Web-based device administration and file management services, as well as a Web, multimedia streaming, FTP, Telnet, SSH, SFTP and RSync servers.

And if all of that isn't enough for you, you can also install any of QNAP's Qpkg applications. Qpkg is a software package management system similar to Linux package managers such as yum and dpkg but, claims QNAP, "QPKG is designed and fine-tuned for running on embedded Linux systems."

Among the packages available under Qpkg are the XMail SMTP server, the Gallery image management application, a terrific systems performance measurement package called iStat (which I'll discuss in a

future Gearhead), OpenLDAP, the Tomcat Java Servlet and JavaServer Pages server, the Asterisk IP telephony system, the Python subsystem, the WordPress blog app, the Joomla content management system and the SqueezeBox streaming audio server.

Anyway, as I discussed last week, after wrestling with a definitely subpar DSL gateway that AT&T had supplied that not only didn't support UPnP but also couldn't be coerced into port forwarding for devices it didn't "see" on the network, I swapped it out for a D-Link DSL-520B ADSL2 gateway and, voila! The QNAP MyCloudNAS wizard found the gateway, used UPnP to configure port forwarding, and everything was



Mark Gibbs' Gearhead

running without any fuss.

I tested remote access via MyCloudNAS to the TS-1079 Pro by logging in from a PC in my son's house in the San Fernando Valley using Teamviewer 6 (an excellent product), and then launching a browser and connecting to the MyCloudNAS subdomain I'd set up. It worked perfectly!

Of course, MyCloudNAS might not be everyone's first choice for Dynamic DNS so the TS-1079 Pro also supports a number of other DDNS services, including dyndns.com and no-ip.com.

As for what else the TS-1079 Pro can do, that is one long list. Beyond delivering really speedy NAS service and running a wide range of applications, the device also provides backup services including Rsync and Time Machine, media serving, IP camera video storage, RADIUS authentication and Syslog service, and antivirus service.

The TS-1079 Pro is really impressive product and, priced at \$2,600 without drives, is great value considering its performance (which is fantastic) and its functionality. I'll give the QNAP TS-1079 Pro a Gearhead rating of 5 out of 5! ■

Gibbs is remote in Ventura, Calif. Access him at gearhead@gibbs.com.

The QNAP TS-1079 Pro delivers really speedy NAS service.



WHY PAY MORE FOR .COM?

--- HURRY! OFFER ENDS 10/31/2011 --- HURRY! OFFER ENDS 10/31/2011 --- HURRY! OFFER ENDS 10/31/2011 ---

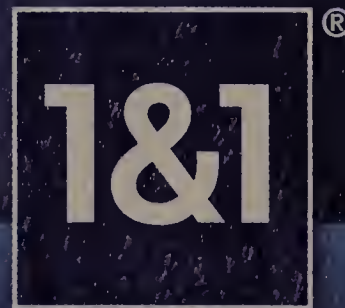
**BEST
VALUE!**

	1&1[®]	GoDaddy[®]	Network Solutions[®]
.com	~~\$9.99~~	\$11.99	\$34.99
ICANN Fee	Included	\$0.18	Included
Private Domain Registration	FREE!	\$9.99	\$9.99
Annual Cost	\$0.99* first year, then \$9.99	\$22.16	\$44.98



YOUR PRIVACY IS IMPORTANT. WE AGREE.

That's why at 1&1, all domains come with **FREE Private Domain Registration** to protect your name, address, phone number and e-mail from spammers and identity thieves.



Get started today, call **1-877-461-2631**

www.1and1.com

* \$0.99 special offer is valid through 10/31/2011. Price is valid for the first year only. After first year, standard pricing applies. Private domain registration is not available for .us, .co, and .ca domains. Visit www.1and1.com for full promotional offer details. Program and pricing specifications and availability subject to change without notice. 1&1 and the 1&1 logo are trademarks of 1&1 Internet AG, all other trademarks are the property of their respective owners. © 2011 1&1 Internet AG. All rights reserved.

GADGETS

Lenovo ThinkPad Tablet a business contender



Keith Shaw's
Cool Tools

THE SCOOP

ThinkPad Tablet

by Lenovo, starts at \$500
(optional keyboard \$100)

► **What it is:** Offered as a tablet for business purposes, the ThinkPad Tablet runs the Google Android 3.1 Honeycomb operating system, and comes with an optional pen with digitizer for customers who want the additional feeling of a stylus for handwriting purposes. Specifications include a dual-core ARM Cortex-A9 processor from Nvidia, a 10.1-inch display, up to 1GB of memory, up to 64GB of SSD storage and integrated front (2 megapixel) and back (5 megapixel) digital cameras. Unlike the Apple iPad, this tablet supports Flash video content, has a full USB 2.0 port and micro-USB slot, as well as a mini HDMI port for displaying on a larger monitor. Network connectivity includes 802.11b/g/n, and it has a SIM slot for 3G wireless access. The optional keyboard plugs in via the USB port and provides a stand for the tablet as well as a protective cover. The full qwerty keyboard provides a better content input experience, and it also includes a ThinkPad "nub" (Lenovo calls it the optical TrackPoint) for mouse navigation (it's fun to see a mouse cursor travel around on a tablet screen).

► **Why it's cool:** Lenovo has done a good job at adding its touch to a standard Android tablet — the ThinkPad includes many preloaded apps out of the box, including Netflix and Documents to Go (for accessing Office documents). The company's Lenovo Launcher on the home screen lets users choose from four main activities (Watch, Email, Listen and Read), with the ability to choose which apps to launch from those activity boxes. An additional Navigation bar along the bottom of the tablet lets users quickly go "back" in an app, go back to the home page or switch between apps quickly (via the Layers button, which is also a nice way of closing open apps). The USB 2.0 slot is a handy way to quickly move files between a PC and the tablet.

► **Some caveats:** I was less impressed with the Lenovo App Shop, which tries to provide users with hand-picked or recommended apps for purchase. In the end it gets confusing between that app store and the Android Market, which provides more apps. The App Shop also made us sign up with a different account name (apart from Google Account access) and credit card information, adding to the confusion. The tablet's short battery life was bothersome, considering a very short power cord

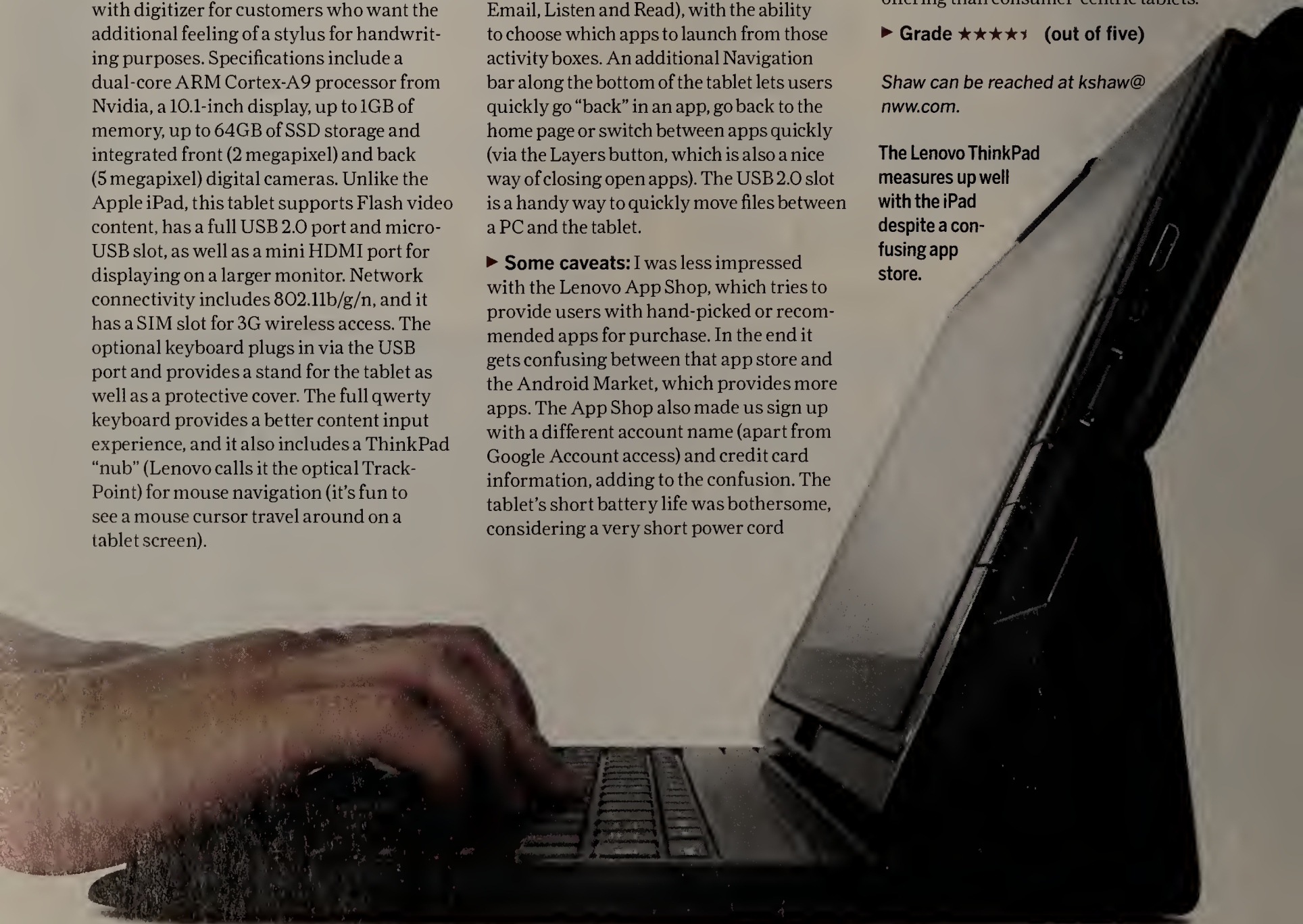
that made it difficult to keep the tablet on a desk (not to mention having to keep a tablet tethered to a power outlet).

► **Bottom line:** The addition of a digitized pen/stylus, keyboard and business-focused apps makes the ThinkPad Tablet a winner for companies considering a more serious offering than consumer-centric tablets.

► **Grade ★★★★★ (out of five)**

Shaw can be reached at kshaw@nww.com.

The Lenovo ThinkPad measures up well with the iPad despite a confusing app store.





www.

**NO
LIFEGUARD
ON DUTY**

.com

WHO'S WATCHING YOUR BUSINESS BETWEEN THE DOTS?

As your business increasingly depends on your network, keeping it safe and available is vital. As the Internet infrastructure company trusted to run .com and .net for more than a decade, Verisign can offer you that confidence with Verisign® DDoS Protection Services. This cloud-based solution continuously monitors and protects your sites, helping to mitigate large-scale distributed denial-of-service (DDoS) attacks. Discover how our industry-leading technology, Internet scale and DDoS expertise can help keep your business connected between the dots.

Download the "DDoS Getting the Attention It Deserves" white paper and keep your site connecting to customers at **VerisignInc.com/guard**.



VERISIGN™

PUBLIC CLOUD SECURITY REMAINS MISSION IMPOSSIBLE



BY CHRISTINE BURNS

**BUT STEADY
PROGRESS IS
BEING MADE
TO ADDRESS
SECURITY
CONCERNS**

Someday, cloud security vendors and cloud services providers will convince enterprise IT that it's safe to move sensitive data and mission critical apps from the private cloud to the public cloud.

Unfortunately, that day has not yet arrived.

Security practitioners, consultants and analysts interviewed for this story say cloud security vendors and cloud services providers have a long way to go before enterprise customers will be able to find a comfort zone in

the public cloud, or even in a public/private hybrid deployment.

When asked for predictions as to when enterprise IT will be willing to go from dabbling in non-sensitive data storage and consuming a little bit of SaaS from trusted entities like Salesforce.com, to running business-critical applications, the answers ranged from six months to two years.

So, what's hindering public cloud adoption?

- Concerns about securing the communications channels within multi-tenant virtual networks.
- Uncertainty about how the exploding number of heterogeneous mobile devices will be securely supported in the cloud.
- An inconsistent path for extending existing identity and access control mechanisms into the cloud.
- Questions on how trusted encryption and tokenization models need to be changed to adequately protect sensitive data stored in the public cloud.

These potential technical issues are compounded by the fact that public cloud providers are notoriously unwilling to provide good levels of visibility into their underlying security practices. For an enterprise, not having a proper window into the security posture of its cloud provider will stall necessary auditing processes and compliance checks.

But all of our sources are confident that eventually public cloud security will reach the level that enterprises currently expect in their privately controlled networks.

The public cloud is past the infancy stage, says Jacob Braun, president and COO of Waka Digital Media, a managed security service provider and consultancy in Massachusetts.

"It's more like a gifted adolescent who's recently moved to a new community. She looks at things a little differently than others. She handles things differently. People are intrigued because she's kind of cool, but at the same time they hold back a bit because she's still a bit unpredictable," Braun says.

But give her just more time and most people are going to want to glom onto her popularity.

Analysts, consultants and customers say they are encouraged by product announcements from established security vendors as well as from startups that address many of these perceived problem spots.

Customers are aware that this conversation about security is taking place before they've been forced to actually jump in, which is a luxurious switch from how security was handled during past corporate computing shifts, like the move to client/server or to the Internet.

"Security administrators simply dealt with the post-deployment security issues as they cropped up," says Gary Loveland, a principal in PricewaterhouseCoopers' Advisory Practice.

With those experiences under their belts, enterprise IT shops are working out the public cloud security issues proactively. "Before they go and add public cloud to the mix, they are asking the right questions that will push their prospective vendors to provide a cloud... that is locked down with most — if not all — the controls they need in place," Loveland says.

A study by the Aberdeen Group's Derek Brink said nearly half of the 110 enterprise IT shops surveyed said they are putting pressure on cloud service providers to implement strong security practices and augmenting that with technology that remains under

enterprise control when the cloud providers' measures seem to come up short.

"Enterprise trust of the public cloud is pretty limited at the moment," says Jon Oltsik, principal analyst at Enterprise Strategy Group. But that mistrust doesn't necessarily reflect any hard evidence that security in the public cloud is bad, he adds.

For example, Oltsik says Amazon "is doing incredible things to build security into its [EC2] infrastructure, to acquire all the proper certifications, hire very talented security personnel" and has upward of 500 security controls in place that should provide some comfort level for enterprise customers.

According to Simon Crosby, former Citrix CTO and founder of Bromium, a startup looking to build products that use virtualization to secure mobile clients, the legal and compliance fears being raised today are remnants of how computing was done 10 years ago.

The public cloud structures being built today are actually far more able to withstand attack than any private network, Crosby says.

"If you told me to go build a secure application, that would run 24 by 7 worldwide and wasn't at risk for data theft I would build something like Netflix, which runs in Amazon's public cloud," Crosby says. "There are 30 billion objects in that store. Go ahead and try to find my stuff in there. And it's so distributed that it can withstand massive DDoS attacks from all sorts of anonymous sources. Yeah, I'd build it in the public cloud. And I wouldn't lose any data."

According to a study written by Phil



Hochmuth, program manager of security products at IDC, users aren't as bullish on that point. When asked if they thought a cloud provider's architecture could be more secure than their own internal one, only one-third of the 500 organizations surveyed said yes.

However, among those that had already jumped into either public or hybrid cloud deployments, more than half of each group agreed that providers offer better security than their respective IT teams.

Richard Reese, manager of EMC's virtual cloud consulting services, suggests there are some enterprise business workloads whose security posture can be greatly improved by pushing them into the public cloud. Take messaging, for example. In IDC's survey, messaging security registered as the most prevalent security SaaS platform employed today. It's used in 30% of the 250 enterprises surveyed and in almost one-quarter of the 250 SMBs.

"IT security administrators have struggled for years to deal with things like automatic digital signing and public/private key encryption for secure email," Reese says. Those security parameters are implemented in the cloud by IT professionals who understand them completely. And they are turned on by default because it's more economical for a provider to consistently manage one highly secure user profile across its customer base.

"So you automatically get that high level of protection [from the cloud] that you may not have been consistently delivering for a variety of business and logistical reasons yourself," he says.

Larry Campbell is vice president of information management and technology at DAI, an international project development firm in Bethesda, Md., with 2,000 development professionals in the field around the world. DAI first built a private cloud to better understand the issues surrounding virtualized computing, then this year completed a move to the public cloud, using multiple providers.

DAI works with NaviSite to run its Oracle databases in the cloud and recently went with Virtustream to host its shared data drives, run a SharePoint portal and manage its messaging services.

There was a lot of back and forth with NaviSite and Virtustream before Campbell was able to make sure the providers' security practices jibed with DAI's internal ones. "But in the end, the reality is that we're a midsize company that

doesn't have a huge IT budget. These [public cloud] providers have deep, technical staffs who have a greater understanding of the security issues in the cloud than we have inside our company," Campbell says.

The proof is in the audit

The public cloud business model hinges on a dynamic environment where it can host many different kinds of workloads that can be moved around at will to optimize the underlying infrastructure. Customers want to make sure there are controls in place to protect their workloads from attacks and want to be able to view information about those controls down to a very granular level.

"But that level of detail is really just outside of the scope of most public cloud providers' business models. Therein lies the disconnect," Enterprise Strategy Group's Oltsik says.

Public cloud providers have been notoriously tight-lipped about details pertaining to their security practices for two reasons. First, they don't want to disclose security practices that give them a competitive advantage, and second, they don't want to risk exposing potential attack vectors.

Sure, some providers give you a pretty dashboard that provides a window into your services running in their cloud. But according to Beth Cohen, senior cloud architect with Cloud Technology Partners, most aren't providing enough information to satisfy enterprise customers. Cohen thinks it is unlikely that the industry will see much of an improvement in this area because "most cloud vendors aren't likely to give away the store."

Cohen thinks it's more likely that cloud providers will continue to turn to third-party certification groups like SAS 70, ISO 2077 and PCI DSS to help provide some piece of mind to their enterprise customers. They can get the certification without having to publicly divulge how they are delivering on their security promises.

Tim Brown, chief security architect for CA's Security Customer Solutions Unit, agrees. "If there is a cloud service provider that has passed all the tests [to earn a publicly recognized certification], it will be far faster for a customer to go with an approved provider than to pursue the certification themselves.

"But we're certainly not at that point, yet," Brown says.

The Cloud Security Alliance (CSA) — a vendor-neutral industry group — is homing in on the issue of cloud provider disclosure with its STAR registry. The CSA holds considerable clout with both vendors and customers because of the yeoman's work it's done to compile and publish guidance documents about cloud security best practices.

The CSA STAR registry is open to all cloud providers and allows them to submit self-assessment reports that document compliance to CSA-published best practices. The searchable registry — which is set to go online this month — will allow potential cloud customers to review the security practices of providers, accelerating their due diligence and leading to higher-quality procurement experiences.

"There is a reasonable middle ground between proprietary security and fair disclosure," and that is the level of information the STAR registry is positioned to collect, says Jim Reavis, CSA's executive director. The CSA matrix asks upward of 200 questions in the areas of compliance, data governance, physical security, human resources security, information security, legal requirements, risk management, release management, resiliency and security architecture.

The question remains, though, how many cloud services provider are going to be willing to pony up the necessary information.

According to CSA Research Director J.R. Santos, the organization is working on vendor participation from two angles. "We are trying to create some friendly competitive pressure on the vendor side and we are hoping that customers will make referring to the STAR registry part of their procurement process to help push the demand."

John Ambra, director of technical services for Modulo, a risk management service provider in Atlanta, works with large enterprise customers to assess the risks involved with taking on new products and services for deployment both in-house and in the cloud.

Whether or not the STAR registry will provide efficient enough information about a cloud provider's environment will be based on what services you're considering, Ambra says.

"If you are just looking to get your help desk tickets, then you are probably fine collecting that level of information. But if you want to use them for credit card transactions, you are still going to do the legwork and do a full-scale on-site assessment," says Ambra. With most public cloud SLA agreements in place today, liability for security issues remains squarely on the customer.



How do I know if my cloud is secure?
How can I ensure my CPU and memory are guaranteed?
Can I get virtual layer 2 networking and a stateful virtual firewall?
How can I ensure global consistency across cloud service providers?

Do I have to re-write or modify my applications?
Can I get flexible role-based access control synchronized with my enterprise directory?
Can I dynamically add memory and CPU to a cloud VM while it is running?
Can I move applications back and forth to the public cloud?
Can I get predictable service costs that still allow me to scale when I need to?
How can I get the cost benefits of multi-tenancy but still access dedicated infrastructure when I need it?

When it comes to the public cloud,
don't just ask questions.
Ask The 10 Big Questions.

VMware vCloud® Datacenter Service

Looking for a public cloud services provider? VMware vCloud Datacenter Service delivers globally consistent enterprise-class cloud computing infrastructure services for your cloud. Offered by VMware-certified service providers, our solution delivers the business agility and cost effectiveness of public clouds without compromising on the portability, compatibility and security demanded by enterprise IT organizations.

Finding the right service provider for your cloud begins with asking The 10 Big Questions.

Start asking at vmware.com/go/the10bigquestions

MORE AND MORE ENTERPRISE IT SHOPS

— as they get comfortable with virtualization practices in their own private clouds — are considering a jump to the public cloud. But before making that leap, consider these pieces of advice from those who have already jumped.

1. Secure your virtual machines

"Hypervisors were never really designed to be running in a public environment," says Beth Cohen, senior cloud architect for Cloud Technology Partners.

That fact doesn't necessarily stop them from being secure, Cohen says. But it does require a more elastic security strategy that can deal with the issues of virtual machines (VM) moving around the underlying infrastructure, interacting with cloud applications and supporting multiple tenants.

Customers going into the public cloud need to understand that perimeter security — while it still needs to be in place — isn't going to help with the internal security of virtual machines, says Michael Berman, CTO of Catbird Networks, a vendor that focuses on virtual machine security.

VMware's vShield offers integrated security services to the underlying VMware hypervisor and a set of APIs that let third-party security vendors build security services on top of VMware's platform. But VMware is only one of the virtualization software vendors

out there and the company has said very little about how these tools will help lock down VMs from Microsoft and Citrix.

2. Lock down endpoints

Predictions for mobile device sales are staggering. Forrester says tablet sales will hit 208 million by 2014. Gartner contends that 1.1 billion smartphones will be sold in 2015. Enterprises moving to the cloud must brace for many more of these consumer-type devices trying to get to corporate data and applications in the cloud.

"The BYOD [bring your own device] to work issue is huge because now you have devices you don't own trying to access your data over networks that you don't control," says Tom Clare, senior director of product marketing at Websense, a content security vendor.

Jacob Braun, president and COO of Waka Digital Media, a managed security service provider and consultancy in western Massachusetts, says one way to help limit the number of users wanting to run personal devices on the corporate network is to set up

policy roadblocks.

These include limiting what users can do on the machine while attached to the network, requiring them to pay for mobile malware protections and confiscating the device if there is a security issue.

But there are legitimate circumstances for giving upper management controlled access through the cloud. Braun's company uses products such as Kaseya's mobile device management module, which is part of the vendor's overall IT System Management platform, to gain that kind of control.



"YOU'VE GOT TO HAVE TEETH IN THE CONTRACT OR YOU'LL HAVE NO LEGS TO STAND ON IF THERE IS A DATA LEAK."

JEREMY CRAWFORD,
CTO, MLSListings

3. Put security in your SLA

Standard cloud service provider service-level agreements (SLA) barely touch on security, so it's a buyer beware situation. "Make sure your provider is willing to move beyond simple monitoring of your service usage," says Torsten George of Agilance, a security vendor that offers governance, risk and compliance services.

"Absolutely push for a custom security SLA," says Jeremy Crawford, CTO of MLSListings, a Silicon Valley-based regional Multiple Listing Service (MLS). Crawford has negotiated security-focused SLAs with three public cloud providers. He takes a look at the providers' standard security agreement, but only consents to about 50% of the language in most cases. He pushes for more favorable language relating to visibility into the providers' systems and sets up specific terms about shared liability should there be a breach.

"You've got to have teeth in the contract or you'll have no legs to stand on if there is a data leak," Crawford says.

4. Act quickly

Richard Reese, manager of EMC's virtual cloud consulting services, says enterprises should move quickly on an overall strategic plan for pushing their business process out to the public cloud in a controlled fashion. By doing so, you avoid rogue pockets of public cloud within the companies.

"I am surprised by how quickly departmental pilot projects morph into business-critical applications," Reese says. Due to the relatively low cost of entry into most public cloud applications, the likelihood that they are being used without IT's knowledge is pretty high.

The number of customers pushing the big public cloud providers to assume some of the liability for security breaches is still very small, contends Michael Berman, CTO at Catbird Networks, a virtual security company in Scotts Valley, Calif.

"Amazon is making a ton of money delivering CPU, bandwidth and storage while assuming none of the liability for the

sensitive data stored there," Berman says. "The economics to make them change that course just aren't in place yet." ■

Burns is a freelance writer and editor in Carlisle, Pa., who has over 15 years experience covering the networking industry. She can be reached at cburns1227@googlemail.com.



Cisco Collaboration Solutions for Mid-size Businesses: **Sophistication. Simplicity. Savings.**



Buy 1 IP Phone— Get a 2nd Free.

US Only. Some restrictions apply.

Learn More at www.cisco.com/go/uc4midsize

Looming threats

CLOUD SECURITY THREATS COME IN ALL SHAPES AND SIZES, so we asked seven experts to weigh in on what they see as the top threat to cloud security. The answers run the gamut, but in all cases, our cloud security panelists believe that these threats can be addressed. ↓

**DOWNTIME DUE
TO A CLOUD OUTAGE**

By Peter Glock,
**CLOUD SERVICE DIRECTOR,
ORANGE BUSINESS SERVICES**

Like a well-tuned symphony orchestra, there is strength in numbers, a collective force to be harnessed to create opportunities for the composer and drive your audience into your concert hall. But sometimes when just one of those players is slightly out of tune, or when your horn section is late for a great performance, the whole orchestra can come to a complete grinding halt.

The same can be said of cloud computing. In the cloud you can leverage the best design, harness flawless operations and leverage the power of the few to benefit the many. However, just like a professional orchestra, the benefits of cloud services can come crashing down on top of you if the cloud is not correctly designed, operated and maintained.



The attraction of the cloud is being on a platform that appears to offer unlimited computing resources. However, the same controls that are managing your enterprise infrastructure are also managing others at the same time, all on the same network. This high-wire act can create a scenario where even a minor glitch or breach could set off a string of consequences. The challenge, then, for cloud providers is whether they can keep on top of a complex and sizable network. The more users on that network, the more difficult it is to troubleshoot, and the greater the likelihood of a cloud blackout that impacts all the infrastructures tied throughout it. Even a successful incident response will likely involve shutting down large parts of the network, impacting you even if your infrastructure is not the source or primary victim of the problem.

Recent headlines have shown this to be true as commercial service providers have experienced wide-reaching cloud outages that have knocked out websites and caused revenue loss for customer and provider alike. However, if you chose wisely, the cloud is still a compelling business proposition.

We see customers adopting a hybrid approach, mixing public cloud services with private, and limiting reliance on a shared platform. In addition, we find that most business operations in the cloud are not mission-critical, so even if an event occurs there is limited loss on the customer side. This is especially evident among large enterprises. Small to mid-size businesses that are dependent on a public cloud for all of their resources are usually the most hurt during an outage.

Operational risk from cloud services can be mitigated through good process management and service-level agreements (SLA) that preserve uptime and provide workarounds in case of downtime. ■



By John Thielens, CHIEF ARCHITECT OF CLOUD SERVICES, AXWAY

The biggest threat in the cloud — certainly for large, mature enterprises — is managing complexity and risk.

When organizations manage on-premise deployments the old-fashioned way, they tend to break down the basic components (network, firewall, storage fabric, computing servers, disaster recovery) and identify the types and levels of risk around each piece — both separately and as part of the entire infrastructure. This way of analyzing an infrastructure generates a tremendous amount of transparency in general, and for risk management in particular.

But when you go to the cloud, elements you typically have been able to analyze for complexity and risk now are being built and managed by someone else, with a potential hit to transparency that can hobble your overall strategy for complexity and risk management.

So enterprises must raise the bar with cloud providers when they are looking to consume cloud-based services. And one key question to ask is: What level of transparency can you offer me (including predictive service-level agreements) so that I can leverage that into my existing risk management directives?

The challenge for cloud providers is to balance the magic of providing a cloud service — which is supposed to deliver a clean, simple, easily consumed interface — with the ability to integrate an enterprise's existing IT fabric. And that includes providing a level of technical disclosure (transparency) that gives enterprises the power to manage the complexity and risk of blending the cloud into their infrastructure. ■

LACK OF VISIBILITY

By Paul Henry, SECURITY EXPERT AND FORENSIC ANALYST, LUMENSION

The biggest threat to cloud security is a lack of visibility, which has opened the door to liability concerns.

Many traditional security providers were late in joining the shift to virtualization and it took years for them to offer solutions that could actually act upon data that flowed seamlessly between virtual machines without physically touching a network interface. In virtualization this has caused a serious lack of visibility and control, which has been further worsened by vulnerabilities or flaws within a neighbor's multi-tenant cloud environment making the liabilities of who is responsible a constant battle.

Given that cloud was built on the promise of being cheaper, we must



now consider that this environment we are creating holds no acceptance of liability on the part of the provider. Providers are offering their cloud services “as is,” without assuming any risk at all, some even providing an exclusion for all liability—leaving anyone facing a cloud security issue without a solution.

What is interesting is that because of these liability issues, providers of cloud will have to institute a security service-level agreement (SLA). Whereas in the past we have been conditioned to accept flaws and vulnerabilities from software vendors, in order for costs to remain low within the cloud environment, providers must now push back on any security-related issues to avoid accepting any potential legal liabilities. ■

EMPLOYEE ‘PERSONAL CLOUDS’

By Simon Crosby,
CO-FOUNDER AND CTO, BROMIUM

When I talk to CIOs about their use of cloud computing, they are focused on building a private cloud—an enterprise-owned, virtualized and automated IT-as-a-service capability that will help them respond more readily to changing business needs, and achieve greater efficiency and availability. Why build a private cloud? The answers are remarkably consistent: Public cloud services are viewed as a security risk.



But there aren't any significant technology barriers to building a public cloud service that is far more secure than any enterprise private cloud. It is easy, for example, to implement a system in which all data is encrypted at rest, and available in decrypted form only to the application consuming it, using keys provided by the enterprise owner of the data (and not the cloud provider).

But the perception remains—driven by the growing stream of reports of successful attacks against companies and governments. The risks are real, and deeply worrying, but the vast majority of cases involve compromise of enterprise private clouds from compromised enterprise PCs.

To restate this: The enterprise is far more vulnerable to attack via its employees and their use of poorly secured enterprise clients than to direct attacks on its data centers. The RSA attack, in which the seeds of RSA tokens were stolen, started with an employee opening an infected Microsoft Excel spreadsheet. The first attack from China on Gmail used a poisoned URL and Internet Explorer 6. So the biggest security threat in the cloud results from the employee's “personal cloud”—the merging of their personal and enterprise interests in a single device with a monolithic OS that fails to isolate and separate different domains of trust. ■

APPLICATION-LAYER DENIAL OF SERVICE ATTACKS

By Rakesh Shah,
DIRECTOR OF PRODUCT MARKETING
AND STRATEGY, ARBOR NETWORKS

The biggest security threat to the cloud is application-layer distributed denial of service (DDoS) attacks. These attacks threaten the very availability of cloud infrastructure itself. If a cloud service is not even available, all other security measures, from protecting access to ensuring compliance, are of no value whatsoever.

Hackers have found and are actively exploiting weaknesses in cloud defenses, utilizing cheap, easily accessible tools to launch application-layer attacks. A major reason they have been successful is that enterprise data centers and cloud operators are not well prepared to defend against them.

Existing solutions, such as firewalls and IPSs, are essential elements of a layered-defense strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS attacks.

As DDoS attacks become more prevalent, data center operators and cloud service providers must find new ways to identify and mitigate evolving DDoS attacks. Vendors must empower data center operators to quickly address both high-bandwidth attacks and targeted application-layer DDoS attacks in an automated and simple manner. This saves companies from major operational expense, customer churn, revenue loss and brand damage. ■

ETHERNET FABRIC IS HERE

Brocade is deploying Ethernet fabric solutions today. From increased automation to more scalable and resilient network architectures, Brocade® Ethernet fabrics flatten your network. In fact, you can manage the entire fabric as one single, logical entity.

A dramatically more automated network.

Reduce complexity and experience a network that works the way you always imagined it should. Brocade Ethernet fabrics enable cloud-optimized networks that make your business more agile. That's why 90% of the Global 1000 already rely on Brocade.

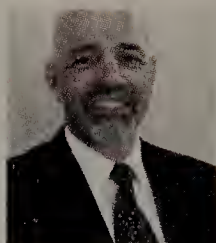
**Find out what Brocade customers already know.
Visit brocade.com/everywhere**



BROCADE

CHANGES IN GOVERNANCE, SECURITY

By Joe Leonard,
SECURITY PRACTICE
MANAGER, PRESIDIO



The two main concerns for cloud security are changes in governance and in operational security.

Organizations must evaluate their existing governance against the cloud security model and understand the residual risks and what compensating controls need to be implemented. Governance areas for concern include risk management, legal and compliance, life-cycle management and portability.

Operational security concerns include business continuity, disaster recovery, incident response, encryption, vulnerability assessment, identity access management and virtualization.

The cloud multi-tenant environment security controls are developed for a general service offering which may or may not provide adequate security for every organization.

Organizations need to assess their vulnerabilities and implement threat prevention policies and technologies; otherwise, reacting to breaches will become more the rule than the exception.

Companies must invest in people with the technical skills necessary

to assess their readiness for implementing different cloud architectures that help move data in and out of public/private clouds and understand the security risks associated with changes related to cloud architecture.

Because of the organizational and cultural complexities of executing cloud strategies, companies are opting to "out task" certain aspects of their operations because skilled resources are in short supply. Companies that understand the organizational impacts of cloud and that can acquire these skills, set the right security policies and build closer relationships with the lines of business will be the best able to mitigate the two big risks associated with cloud security. ■

LOSS OF CONFIDENTIAL DATA

By Guy Helmer
CTO, PALISADE SYSTEMS

Confidentiality of content is the top cloud security threat.

Companies of all sizes and across all industries have taken steps to protect confidentiality of their content in their legacy data centers because of high costs from disclosures, penalties resulting from breaches, and loss of reputation.

However, in the cloud, content can't be monitored, controlled and protected as easily, because of lack of visibility, sharing systems with other cloud customers, and potential for malicious insiders at cloud providers.

Cloud environments pose different obstacles for safeguarding content. In information-as-a-service (IaaS) environments, customers have

the ability to create corporate infrastructure in the cloud. Encryption, access control and monitoring can reduce the threat of content disclosure. However, modern content security monitoring and filtering solutions may be difficult or impossible to deploy due to architectural or other limitations in this cloud environment.

In platform-as-a-service (PaaS) environments, customers can quickly spin up new Web, database and email servers, but will find they have even fewer ways to do any monitoring or protection of content than in an IaaS environment.

Customers with confidential content are at the greatest mercy of vendors in SaaS environments. With few exceptions, there is no way for a customer to ensure security of content at a SaaS provider — the SaaS provider must be completely trusted and trustworthy to maintain security on behalf of the customers. ■

Where to become a cloud security expert

NICHE VENUES

The Cloud Security Alliance (CSA) is hosting CSA Congress 2011 in Orlando on Nov. 16 and 17. The CSA is a vendor-neutral organization that is largely credited with driving best practices in cloud security across the industry.

Salesforce.com, one of the more trusted public cloud SaaS applications, holds its annual conference called Dreamforce in September.

An organization called **CloudCamp** bills itself as an "unconference" and is a series of regional venues where early adopters of cloud computing technologies gather regionally to exchange ideas. In the fourth quarter of 2011, there are upward of 15 events planned around the world.

SANS, an information security training organization, has established a new line of courses on cloud security that include "Cloud Security Fundamentals" and "Virtualization and Private Cloud Security" — both of which are slated to take place in New Orleans in January 2012.

BIG SECURITY CONFERENCES

First up in North America is **RSA** in San Francisco in February 2012. RSA is holding its European conference in London this week and in Beijing in November.

Several users said that if you really want to know the state of security in the cloud, you should attend the **Black Hat conference**, which next will take place in late July in Las Vegas.

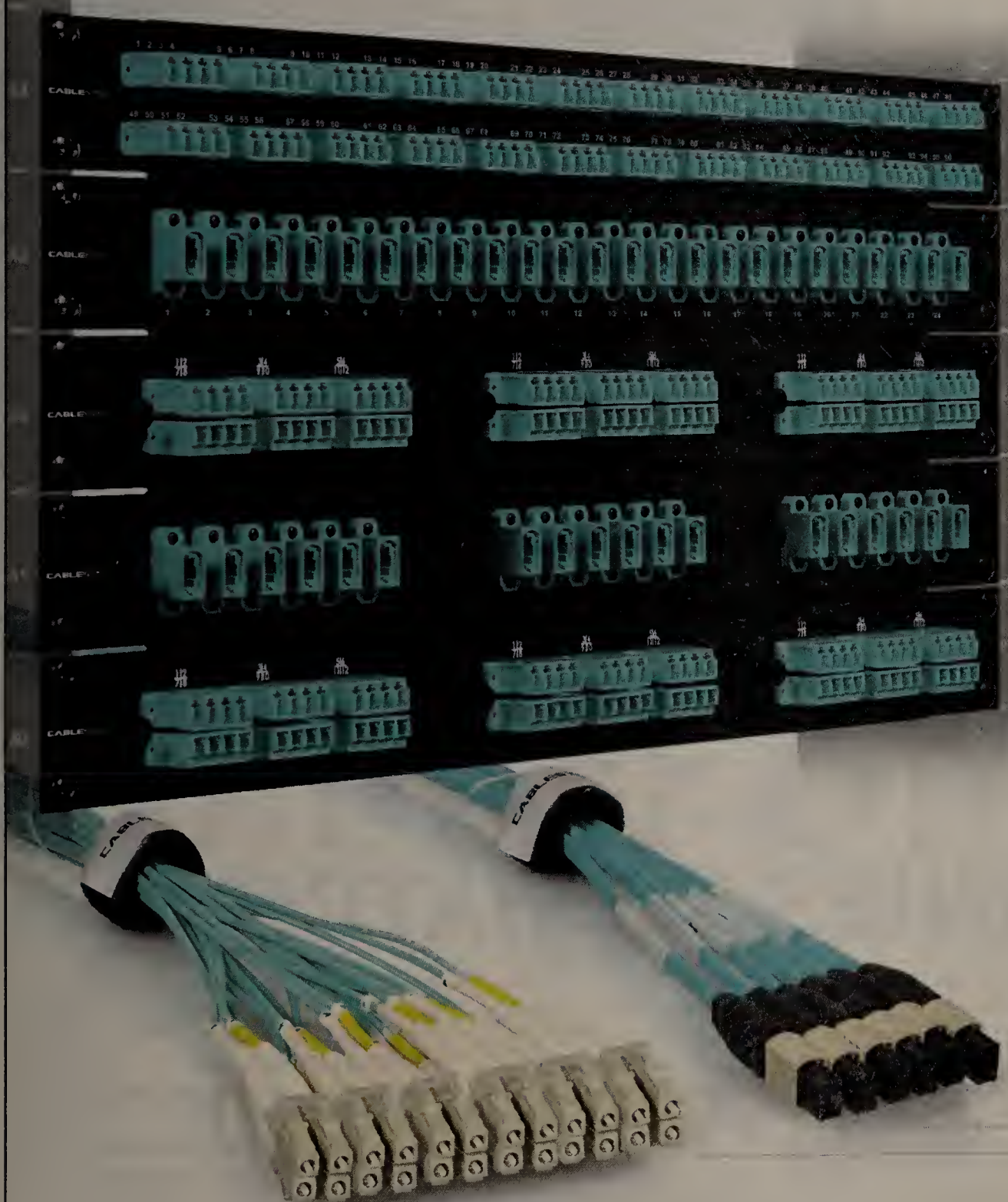
ON THE WEB

Ed Halletky is owner of the analyst firm Astro-Arch Consulting. Halletky's blog appears on the site **TheVirtualizationPractice.com**. He writes under the pseudonym Texiwill.

A second popular blog is called **Rational Survivability** and written by **Chris Hoff**, who describes himself as a security professional with "20 years of experience in high-profile global roles in network and information security architecture, engineering, operations, product management and marketing with a passion for virtualization and all things Cloud." He's employed by Juniper Networks, but his opinions are his own.

Need a High Speed Fiber Network?

— 10G • 40G • 100G —



LC Quad Patch Panel
96 Fibers

MPD Patch Panel
288 Fibers

LC Quad Adapter Panels
72 Fibers

MPD Adapter Panels
216 Fibers

LC Quad MPD Cassettes
72 Fibers

Plug and Play Bundled Cables for
10G/40G/100G Applications
OM3/OM4

10G/40G/100G HD Solutions

Cablesys designs and builds a series of 1 RMU High Density (HD) fiber panels to maximize output. With LC or MPD, we can fit up to 288 fibers in one RMU to support your 10G or 40G/100G applications (IEEE802.3ba). We also build bundled fiber cables in any length, any size and any configuration with custom labeling. All you have to do is plug, and play. No fiber cutting, polishing or terminating to mess up your delicate datacenter. Give us a call, you will be surprised how easy it is.

cablesys.com/nw

800.555.7176

cs@cablesys.com

CABLESYS

CLOUD SECURITY

COMPANIES TO WATCH

BY CHRISTINE BURNS

Security is one of the major impediments to enterprises moving their resources into the cloud. So it's not surprising that numerous cloud security companies are springing up, attempting to address specific cloud security issues, like protecting virtual machines or encrypting data in motion. Here are five up-and-coming companies — some still in stealth mode — that hold a great deal of promise.

Bromium

CUPERTINO, CALIF., AND CAMBRIDGE, U.K.

What it offers: Still in stealth mode, but founders have hinted they are building a product that uses virtualization to help secure all types of endpoints.

How much it costs: No pricing available at this time.

Who heads the company: Its founders are Gaurav Banga, the former CTO of Phoenix Technologies; Simon Crosby, the former CTO of the Data Center and Cloud Division of Citrix; and Ian Pratt, the current chairman of Xen.org and another Citrix veteran.

Why it's worth watching: Crosby is one of the more outspoken proponents of public cloud computing. He contends the security

threats to cloud computing don't grow out of inherent holes in the cloud, but rather stem from unprotected clients, like the ones enterprise users are adding to corporate networks at alarming rates. While the company — which picked up \$9.2 million in venture capital money early this past summer — won't be divulging product details until later this fall, Crosby has gone on record as saying that the primary benefit of virtualization will be security. It will be a neat trick if the company can pull it off.

CipherCloud

CUPERTINO, CALIF.

What it offers: Cloud data encryption and tokenization.

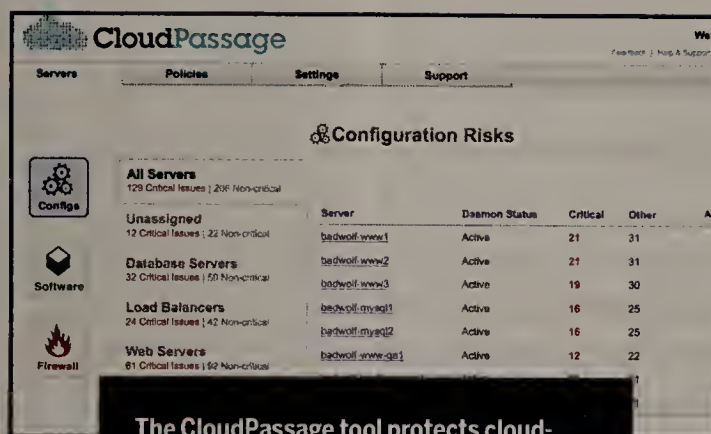
How much it costs: \$20 per user per month.

Who heads the company: Pravin Kothari is founder and CEO. Prior to starting up CipherCloud, Kothari was founder, CTO and interim CEO of Agilience, a GRC software company, and was co-founder and vice president of engineering at ArcSight, a security and compliance vendor.

Why it's worth watching: CipherCloud is attempting to take on encryption and tokenization in a way that protects data both at rest and in motion. It also has low performance overhead for SaaS applications, and does not require enterprise customers to hand over control of encryption keys to their cloud service providers.

According to Kothari, the CipherCloud gateway is a lightweight software appliance that encrypts and decrypts data and attachments as they pass through it. It does so in real time without loss of performance, format or functionality of the application.

"Our gateway is designed as a stateless solution. This, along with our high-performing encryption algorithms, ensures near-zero impact on the performance," Kothari says. In fact, in certain configurations where CipherCloud has switched on static caching, Kothari says the company has seen improvements in performance with its gateway in the middle.



The CloudPassage tool protects cloud-based virtual machines.

CloudPassage

SAN FRANCISCO

What it offers: Halo SVM and Halo Firewall SaaS products, both of which aim to lock down virtual servers.

How much it costs: Free.

Who heads the company: Co-founders are Carson Sweet (serving as CEO), Talli Somekh (executive chairman) and Vitaliy Geraymovych (vice president of engineering). They came to CloudPassage from GlobalNetXchange (now Agentrics), Musea Ventures, and the technology consulting field, respectively.

Why it's worth watching: Sweet argues that virtual machines enabled the explosion in cloud computing, "but people sometimes sort of forget about the virtual network around those machines that need to be secured." CloudPassage focuses on securing the virtual server environment, which is widely viewed as one of the most unpredictably vulnerable spots in the cloud. Early this year, the company released two free services designed to protect cloud-based virtual servers by maintaining firewall policies (Halo Firewall) and checking for vulnerabilities (Halo SVM). The company plans to charge for higher-level VM security services.

High Cloud Security

MOUNTAIN VIEW, CALIF.

What it offers: Virtual machine encryption solutions.

How much it costs: Not available yet.

Who heads the company: Co-founders are Bill Hackenberger and Steve Pate. Hackenberger, who serves as CEO and president,

has founded three other startups, one of which, AIM Technology, was bought by Network General. He has also served as vice president of engineering at both Caymas Systems and Vormetric. Pate, who serves as CTO, held that same position at encryption vendor Vormetric and worked at virtualization vendor HyTrust.

Why it's worth watching: High Cloud Security recently printed an excerpt from an article published in 2010 that outlined in three easy steps how to hijack a virtual machine and in the process steal sensitive data that might be running on the VM at that point in time. High Cloud says the way to prevent this from happening is to encrypt everything at the storage layer that may contain sensitive information. The company's yet-to-be-released product is currently in beta testing.

HyTrust

MOUNTAIN VIEW, CALIF.

What it offers: The HyTrust Appliance (currently available version is 2.2) provides centralized access control for virtual servers, providing enforcement of security policies and compliance controls.

How much it costs: \$1,000 per host supported.

Who heads the company: John De Santis, formerly vice president of cloud services at VMware, is CEO. Co-founders are Eric Chiu and Renata Budko, who are president and vice president of marketing, respectively. Hemma Prafullchandra is CTO. She was formerly CTO of FuGen Solutions, a managed provider of federated identity interoperability and compliance service.

Why it's worth watching: We've been tracking HyTrust for two years now, since it was selected as a 2010 company to watch and won best of show accolades at several industry trade shows. The product held its own against established market leader Trend Micro in our recent test of virtualization security management tools. The company has reportedly closed more business in the first two quarters of 2011 than it did in the whole of 2010. ■

■ Editorial Index

Agentrics	31
Agilience	22, 31
Amazon	4, 19, 34
Apple	4, 6, 16, 34
Arbor Networks	26
ArcSight	31
AT&T	14
Bromium	19, 26, 30
CipherCloud	31
Cisco	3, 6-7, 10
Citrix	19, 22, 30
Cloud Technology Partners	20, 22
CloudPassage	31
D-Link	14
EMC	20, 22
Enterasys	10
FuGen Solutions	31
Google	7, 16, 34
High Cloud Security	31
HP	3, 10
Huawei	10
HyTrust	31
Juniper Networks	10, 28
Lenovo	16
Lumension	25
Microsoft	6-7, 22, 26
MicroStrategy	6
MobileIron	7
Musea Ventures	31
Network General	31
Oracle	20, 34
Palisade Systems	28
Phoenix Technologies	30
Presidio	28
QNAP	14
RSA	26
Salesforce.com	19, 28, 34
Trend Micro	31
VMware	22, 31
Vormetric	31
Xen.org	30

■ Advertiser Index

Advertiser	Page #	URL
1&1 Internet AG	12-13, 15	www.1and1.com
Brocade Communications Systems	27	brocade.com/everywhere
Cablesys	29	cablesys.com/nw
CenturyLink	35	centurylink-business.com
Cisco Systems	23	www.cisco.com/go/uc4midsize
Dell Inc	2	DellStorage.com/GetFluid
IBM Corp	36	ibm.com/facts
Microsoft Corporation	11	Microsoft.com/office 365
NetSupport Inc	33	www.netsupportmanager.com
Sensaphone	33	www.sensaphone.com
SonicWALL	5	sonicwall.com/optimize
VMware Inc	21	vmware.com/go/the10bigquestions
Verisign Inc	17	VerisignInc.com/guard
dtSearch Corp	33	www.dtsearch.com

These indexes are provided as a reader service. Although every effort has been made to make them as complete as possible, the publisher does not assume liability for errors or omissions.

*Indicates Regional Demographic

International Data Group

CHAIRMAN OF THE BOARD: Patrick J. McGovern

IDG Communications, Inc.

CEO: Bob Carrigan

Network World is a publication of IDG, the world's largest publisher of computer-related information and the leading global provider of information services on information technology. IDG publishes over 300 computer publications in 85 countries. One hundred million people read one or more IDG publications each month. Network World contributes to the IDG News Service, offering the latest on domestic and international

computer news.

Publicize your press coverage in Network World by ordering reprints of your editorial mentions. Reprints make great marketing materials and are available in quantities of 500 and up. To order, contact the YGS Group, (800) 290-5460 ext. 148 or e-mail networkworld@theygsgroup.com.

Network World Events and Executive Forums produces events including IT Roadmap, DEMO and The Security Standard. For complete information on our current event offerings, call us at 800-643-4668 or go to www.networkworld.com/events.

Periodical postage paid at Framingham, Mass., and additional mailing offices. Posted under Canadian International Publication agreement #PM40063731. Network World (ISSN 0887-7661) is published twice monthly except for monthly in July by Network World, Inc., 492 Old Connecticut Path, P.O. Box 9002, Framingham, MA 01701-9002. **Network World** is distributed free of charge in the U.S. to qualified management or professionals. To apply for a free subscription, go to www.subscribe.nw.com or write Network World at the address below. No subscriptions accepted without complete identification of subscriber's name, job function, company or organization. Based on the information supplied, the publisher reserves the right to reject non-qualified requests. Subscriptions: 1-877-701-2228. Nonqualified subscribers: \$5.00 a copy; U.S.—\$129 a year; Canada—\$160.50 (including 7% GST, GST#126659952); Central & South America—\$150 a year (surface mail); all other countries—\$300 a year (airmail service). Digital annual subscription rate of \$29.00. Four weeks notice is required for change of address. Allow six weeks for new subscription service to begin. Please include mailing label from front cover of the publication. Network World can be purchased on 35mm microfilm through University Microfilm Int., Periodical Entry Dept., 300 Zebb Road, Ann Arbor, Mich. 48106. **PHOTOCOPYRIGHTS:** Permission to photocopy for internal or personal use or the internal or personal use of specific clients is granted by Network World, Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of \$3.00 per copy of the article, plus 50 cents per page is paid to Copyright Clearance Center, 27 Congress Street, Salem, Mass. 01970. **POSTMASTER:** Send Change of Address to Network World, P.O. Box 3090, Northbrook, IL 60065. Canadian Postmaster: Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A7C9. Copyright 2009 by Network World, Inc. All rights reserved. Reproduction of material appearing in Network World is forbidden without written permission. Reprints (minimum 500 copies) and permission to reprint may be purchased from The YGS Group at (800) 290-5460, ext 100, or networkworld@theygsgroup.com. USPS735-730



■ Network World, Inc.

492 Old Connecticut Path,
P.O. Box 9002
Framingham, MA 01701-9002
Phone: (508) 766-5301

To Send E-Mail to NWW Staff

firstname_lastname@nww.com

CEO: Mike Friedenberg

SVP, CHIEF CONTENT OFFICER: John Gallant

SVP, GROUP PUBLISHER: Bob Melk

PUBLISHER: Andrea D'Amato

Online Services

SVP, GM ONLINE OPERATIONS: Gregg Pinsky

NATIONAL DIRECTOR, DIGITAL SALES: Elisa Della Rocco

MANAGER, ONLINE ACCOUNT SERVICES: Danielle Tetreault

Custom Solutions

SVP STRATEGIC PROGRAMS &

CUSTOM SOLUTIONS GROUPS: Charles Lee

Events

SVP, EVENTS: Ellen Daly

DIRECTOR OF EVENT OPERATIONS: Deb Begreen

Marketing

VP MARKETING: Sue Yanovitch

Ad Operations

SENIOR PRODUCTION MANAGER: Jami Thompson

Finance

VP FINANCE: Mary Fanning

Human Resources

SVP HUMAN RESOURCES: Patricia Chisholm

Circulation/Subscription

CIRCULATION MANAGER: Diana Turco, (508) 820-8167

IDG List Rental Services

DIRECTOR OF LIST MANAGEMENT: Steve Tozeski

TOLL FREE: (800) IDG-LIST (US only)/

Direct: (508) 370-0822

■ Sales

Northeast/Midwest/Central

ACCOUNT DIRECTOR, INTEGRATED SALES:

Timothy Keough, (508) 766-5475

Southeast/Mid-Atlantic

REGIONAL ACCOUNT DIRECTOR:

Jacqui DiBianca, (610) 971-0808, FAX: (201) 621-5095

Northern California/Northwest

ACCOUNT DIRECTOR, INTEGRATED SALES:

Patti Sellman, (415) 267-4522

Silicon Valley/Southwest/Rockies/Utah

ACCOUNT DIRECTOR, INTEGRATED SALES:

Coretta Wright, (415) 267-4515

Marketplace/Emerging Markets—National

ACCOUNT MANAGER, EMERGING MARKETS:

Enku Gubaie, (508) 766-5487

ONLINE

Northeast/Midwest/Central

ACCOUNT DIRECTOR, DIGITAL SALES:

Melissa Rocco, (508) 766-5491

East

ACCOUNT DIRECTOR, INTEGRATED SALES:

Jacqui DiBianca, (610) 971-0808

Northern California/Northwest/Rockies/Utah:

ACCOUNT DIRECTOR, DIGITAL SALES:

Katie Layng, (415) 267-4518

Northern California/Southwest

ACCOUNT DIRECTOR, DIGITAL SALES:

Katie Albang, (415) 267-4510

Custom Solutions

EASTERN SALES DIRECTOR: Brett Ferry, (508) 988-6941

WESTERN SALES DIRECTOR: Karen Wilde, (415) 267-4512

■ Event Sales

DEMO

SVP, DEMO: Neal Silverman, (508) 766-5463

IT Roadmap

ACCOUNT DIRECTOR, EVENT SALES, WESTERN REGION:

Brian Klunk, (415) 267-4514

ACCOUNT DIRECTOR, EVENT SALES, EASTERN REGION:

Michael McGoldrick, (508) 766-5459

WHILE YOU WERE OUT
 For: You Time: Middle of the night
PROBLEM:
 Server went down ☒ Power failure ☒
 Water on floor ☒ Temperature High ☒

Now with
**Wireless
Sensors**

Did you get
the message?

Sensaphone Remote Monitoring Products
 use *redundant communication paths, built in battery backup, and supervised sensors* to make sure that when something goes wrong in your computer room *you get the message.*

Notification Via:

- Voice Phone Call • E-Mail
- Text Message • SNMP Trap
- Pager • Fax



Get your **FREE** application guide now

SENSAPHONE®
 REMOTE MONITORING SOLUTIONS

877-373-2700
www.sensaphone.com

MADE IN THE
USA

The Smart Choice for Text Retrieval® since 1991

dtSearch®

Instantly Search Terabytes of Text

With dtSearch: "Endless indexing is now a breeze" – *Computerworld*

"Impressive searching power ... handles more than a terabyte of text in a single index" – *Network World*

"Lightning fast ... performance was unmatched" – *Redmond Magazine*

For hundreds more reviews & developer case studies, see www.dtSearch.com

Highlights hits in a wide range of data, using dtSearch's own file parsers and converters

- Supports MS Office through 2010, OpenOffice, ZIP, HTML, XML/XSL, PDF and more
- Supports popular email formats, including nested and ZIP attachments
- Spider supports static and dynamic web data
- API for SQL-type data, including BLOB data

25+ full-text and fielded data search options

- Federated searching; advanced data classification objects

APIs for C++, Java and .NET through 4.x

- Native 64-bit and 32-bit Win / Linux APIs; .NET Spider API
- Content extraction only licenses available

Desktop with Spider

Network with Spider

Publish (portable media)

Web with Spider

Engine for Win & .NET

Engine for Linux

Ask about fully-functional evaluations!

www.dtSearch.com 1-800-IT-FINDS

PC Remote Control

Internet Gateway

Thin and Zero Client Support

Chat and Audio

Workstation Monitoring

NetSupport
www.netsupport-inc.com

TOP 100 **BEST IN TECH 2011**

Power in your hands!

NetSupport Manager
Remote Control for Any Platform

Remote Control for Any Platform

Web Based Helpdesk

IT Asset Management

Desktop Security

Powerful Desktop Alerting

Classroom Monitoring for Mac & Linux

Classroom Management for Windows

IT teams are constantly under pressure to do 'more with less' - less manpower, less resources, less budget. But the support demands of the modern, dispersed business environment are greater than ever.

With comprehensive multi-platform support for Windows, Linux, Mac and, crucially, mobile, combined with advanced desktop management functionality, NetSupport Manager remote control software gives helpdesk professionals the power to support more systems and users - whatever the platform, whatever the location.

To see why 72,000 organizations manage over 9,000,000 computers each day with NetSupport Manager remote control software,
Download a free 30-day trial today.

w: www.netsupportmanager.com e: sales@netsupport-inc.com
 t: 1-888-665-0808 (Toll Free)



IT — as Steve said, “Click. Boom. Amazing!”

I WILL not be writing at length about Steve Jobs in this column because many other people are doing so and some of them far better than I ever could. All I’ll say is that he was unique and the computer industry has lost an icon, a force and, to many, a hero.

So, what I want to discuss this week is an idea that Jobs’ company, Apple, once used extensively in their advertising: Think different.

But what does it mean to “think different”? Apart from being essentially ungrammatical, the phrase evokes the idea of bucking the system, not following the trends, taking the path untraveled, boldly going where no man ... no, that was something else ... all of which is great in theory but really hard in practice.

The fact is that in IT, thinking “different” happens a lot. You get handed a problem and immediately a dozen solutions come to mind that range from spending vast amounts of money through to changing the laws of physics, but more often than not, it’s “bandage” time because the biggest constraint is history.

History matters when IT has to solve problems because IT rarely has a “green field” situation. The reality of most IT organizations is that you can’t implement a complete makeover to fix all of the big issues, yet fixing the core problems can’t really be done without hitting the “reset” button!

But what to do? Don’t just think different, act “different” ... be crazy (and you might want to watch Steve Jobs narrating “The Crazy Ones” from 1997, tinyurl.com/6l67qg5). Instead of the usual “we can’t,” go for the “we could if ...”

The pragmatic version of thinking different is more about attitude

than reality ... it’s “could do” over “can’t do.” The reality is that you have a limited budget and they (the department making your life less enjoyable) have needs that can’t be satisfied given the circumstances.

Of course, that department thinks you can work miracles and, it goes without saying, you can! But you need resources and they need to understand that your limitations are not your choice but a grim reality of economics and business politics.

So, once again, we come back to the issue of selling IT to the organization. The central idea is that IT is not an overhead like the free soft drinks machines or the bucket of doggie milk bones beside the receptionist’s desk.

But neither is IT the Hogwarts of tech. You can’t conjure systems and services out of thin air and no one should ever make the mistake of thinking you can. Make the majority of your IT miracles prosaic and pedestrian and then, when it matters, you can pull the rabbit out of the hat (just make sure the rabbit is a rare occurrence but not too rare).

If you want IT to be treated as an integral part of the organization rather than being seen like air conditioning or janitorial service, you have to learn to think and speak different about how you express what IT does and can do.

So, as Jobs was wont to say, “one more thing” about thinking and acting different: Maybe you need to learn to channel Jobs and position IT as Steve would have positioned, say, the next iPhone: As the greatest thing ever! As Steve said in the Macworld keynote in 2006, “Click. Boom. Amazing!” ■

Gibbs is saddened in Ventura, Calif. Notes to backspin@gibbs.com.



3 small items from the week we lost a giant

SEEMINGLY ENDLESS coverage of his passing last week offered the public an opportunity to learn everything it could

ever want to know about Steve Jobs, including what would appear to be his favorite photograph ... of himself.

The latter required connecting a couple of dots. The morning after Jobs’ death, I got to wondering about the status of his upcoming authorized biography, so I went to Amazon, where a forum contributor had noted that both the book cover and Apple’s homepage tribute to Jobs were using the same photograph. Searching a bit more, I learned that it’s a picture Apple has used for years.

That the photo had been chosen for both the cover and Apple’s homepage might be a coincidence, I thought, but to even entertain that possibility you’d have to believe that Jobs was a man who didn’t bother himself with details.

Benioff vs. Ellison

Before the week turned somber, Salesforce.com CEO Marc Benioff and Oracle CEO Larry Ellison had been providing comic relief with their slapstick battle at the Oracle OpenWorld conference in San Francisco.

Benioff was there to deliver a Wednesday keynote address, but couldn’t resist tweeting a few jabs at Ellison earlier in the week. Before you could say “junior high school,” Ellison dropped a fail

whale on Benioff by bouncing him off the conference agenda. Oracle claimed it was an unavoidable “scheduling change.”

C’mon, guys, strap on the gloves and get in the ring; put it on pay-per-view and raise a fortune for charity. I’d pay to see it.

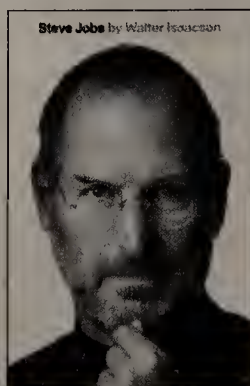
Page reappears on Google+

It had become a media-driven tempest — “Hey, look, Google CEO Larry Page has stopped using Google+” — and, truth be told, this one got rolling on Buzzblog when I noted Sept. 16 that Page had not posted publicly on his social network for a month. While I was careful to note that an absence of public posts didn’t mean Page had abandoned Google+ altogether, others were less nuanced.

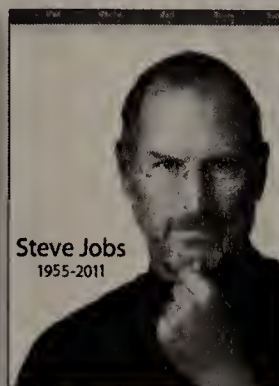
After remaining publicly silent for another 12 days, Page finally tossed the masses a bone. Among the hundreds of comments left on his post were: “Welcome back to Google+ Mr. Page.” ... “Glad to see you here again!” ... And, “You didn’t dump Google+ after all.”

My initial point was that Page shouldn’t have set up shop on Google+, been Mr. Chatty for a couple of weeks, and then gone publicly silent without explanation. That should be even more evident now that his base of followers, then 300,000, now tops a half-million. And they’re clamoring to hear from him. ■

I want to hear from you, too. The address is buzz@nww.com.



Book cover, left; Apple homepage.



Delivering a stronger network. And more personal service.

Our network has expanded, and so has our ability to serve you. When you combine our personal, consultative approach with our premiere technology platform – including colocation, managed hosting and nationwide fiber-optic network with global reach – you will find you are free to drive productivity and bottom-line growth. **Your link to what's next.**

Data | Voice | Managed Services



CenturyLink™
Business

See the benefits of partnering
with us at centurylink-business.com

Qwest is now CenturyLink.



Virtualize more with WebSphere. Or pay more with WebLogic.

Over 400 highly logical reasons to choose IBM WebSphere® over Oracle WebLogic®:

1. Save 57% on first-year licensing and support.
2. Choose from more virtualization options (including VMware and Xen).
3. Pay only for cores you use (not always true with Oracle WebLogic).
- 4–404. Be in good company (last year, over 400 Oracle WebLogic clients chose IBM WebSphere).

ibm.com/facts

SAVINGS based on publicly available information as of 6/13/2011 comparing Oracle WebLogic Server Enterprise Edition to IBM WebSphere Application Server Network Deployment, both on an IBM Power 730 Express server (2 chips, 8 cores each). IBM, the IBM logo, ibm.com, WebSphere, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. © International Business Machines Corporation 2011.